UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STEPHANIE HOFFMANN, Individually an On Behalf of All Others Similarly Situated,

Plaintiff,

Civil Case No.

-against-

MAJOR MODEL MANAGEMENT, INC.,

Defendant.

CLASS ACTION COMPLAINT

Plaintiff STEPHANIE HOFFMANN, individually and on behalf of all others similarly situated, alleges the following against MAJOR MODEL MANAGEMENT, INC., based on personal knowledge with respect to herself and on information and belief as to other allegations:

INTRODUCTION

1. When fashion models seek representation and management, they put their trust in the companies that promise to take reasonable precautions to protect their sensitive personally identifiable information ("PII"). Defendant, MAJOR MODEL MANAGEMENT, INC., ("MMMI") violated that trust.

2. MMMI collected and stored massive PII of Plaintiff and each member of the proposed class. MMMI failed to safeguard their clients' PII. MMMI failed to properly implement and maintain materials and privacy statements. MMMI failed to comply with industry standards, best practices, and state laws. As a proximate result, third parties gained unauthorized long-term access to the PII of Plaintiff and every class member.

3. Plaintiff and each member of the proposed class have suffered injury and pecuniary loss. In addition to the clear injury that any victim of a data breach suffers by virtue of the breach

itself, Plaintiff claims fraud, identity theft, temporary loss of use of their social security numbers, passports, bank accounts, credit or debit cards, and loss of time and money monitoring her finances for future fraud.

4. Upon information and belief, the Plaintiff's stolen/hacked PII is being sold on the dark web, a seedy corner of the internet where illicit black markets thrive.

5. Plaintiff brings this suit to recover their losses caused by MMMI's failure to keep her PII secure and to force MMMI to improve its data security practices and protocols.

PARTIES

6. Plaintiff, STEPHANIE HOFFMANN, is an individual residing in Old Greenwich, CT who was a contract fashion model with MMMI from 2015 to 2018, and whose PII was compromised in the Data Breach.

7. Defendant, MMMI, is a New York corporation with its principal place of business located at 344 West 38th Street, New York, New York 10018.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are more than 100 individual members of the proposed class, their claims exceed the sum or value of $5,000,000, exclusive of interests and costs, and some members of the proposed class are residents of different states than Defendant.

9. This Court has jurisdiction over Defendant because MMMI is a New York corporation, subject to general jurisdiction in New York; many of the wrongful acts alleged in this Complaint took place in New York, such that the exercise of jurisdiction by this Court is necessary and proper.

10. This court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367(a).

11. Venue is proper in this District under 28 U.S.C. §1391 (b) and (c) because a substantial part of the acts or omissions giving rise to this action occurred in this District and Defendant is subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

A. Plaintiffs' Agency and Management Agreement with MMMI.

12. MMMI is engaged in the business of fashion model management. The company provides traditional, full-service fashion model and talent management services, specializing in the representation and management of models, entertainers, artists, athletes and another talent to various clients which includes retailers, designers, advertising agencies, print and electronic media and catalog companies.

13. On July 30, 2015, Plaintiff HOFFMANN entered into an Agency and Management Agreement with MMMI.

14. The AGREEMENT provided, in pertinent part, that Plaintiff was engaging MMMI as their sole and exclusive personal manager in New York "in connection with the development of Plaintiff's career in modeling, advertising, licensing, entertainment, musical, theatrical,dramatic,artistic,fashion,film,video,television,CD-ROM,social network industries (such as Facebook,MySpa,Twitter,Tumblr,Instagram,blogs,etc.) and other visual media industries, and all services."

15. The AGREEMENT contains a Registration Form which Plaintiff and members of the proposed class are required to complete manually. This form requests place of birth, date of birth, nationality, permanent address, cell number, email address, social security number,

signature, passport number and visa number. The form contains an instruction to "attach a copy of the social security card and passport" to the AGREEMENT.

16. Where applicable, the AGREEMENT sets forth information about the contracting party's bank account number and instructions for direct deposit transactions.

17. The AGREEMENT contains an Acknowledgement Clause that states that MMMI may use and transmit the contracting party's "name, personal information, images and/or likeness for the purpose of facilitating my participation on the Web."

18. At all relevant times, MMMI owned, operated and maintained a Website at https://www.majormodel.com. MMMI stores massive amounts of models' PII on their servers and utilizes this information to maximize their profits through predictive marketing and other marketing techniques.

19. This Website permits a search for specific MMMI male and female fashion models and offers access to their photos and related information, such as age and physical attributes.

20. At all relevant times, the Website did not contain a privacy policy, cookie policy or data use policy.

21. On August 25, 2020 MMMI served a notice on Plaintiff that states as follows:

> We at Major Models value your privacy and respect the right to keep your information private, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information. Over this past weekend, from approximately August 22 to August 23, Major Models' website was hacked in an attack wherein some past and present models contracting information was made accessible to third parties who breached Major Models' industry leading website security protocols. To our knowledge, this data breach only affected a very small number of models and within hours of being made aware of this issue, Major's technology and security department rectified the hack and any surrounding issues.

22. Upon information and belief, the data breach has been continuous since at least May 27, 2020.

23. Upon information and belief, the data breach affects at least 500 current and former fashion models whose PII was made accessible to third parties and the general public via the MMMI Website.

24. The data breach consists of PII disclosure of the place of birth, date of birth, nationality, permanent address, cell number, email address, social security number, signature, passport numbers and visa numbers.

25. The data breach consists of PII disclosure of actual copies of social security number cards, passports, and visas.

26. Plaintiff sustained loss and pecuniary injury because her PII was compromised in the Data Breach which consisted of disclosure of her place of birth, date of birth, nationality, permanent address, cell number, email address, social security number, signature, passport numbers and actual copies of her social security number card and passport.

27. This data breach affects all former and current fashion models who are or were featured on the website http://www.majormodels.us ,and whose PII was compromised as a result of MMMI'S failure to: (i) adequately protect its users PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor and control those on MMMI'S network that present a threat.

28. All private profiles, contracts, financial information, confidential and sensitive personal information of Plaintiffs and proposed members was publicly searchable by anyone in the World for at least four [4] consecutive months and probably more.

29. Plaintiff and proposed class members were never given an "opt out" option or privacy settings to prevent such disclosure of their PII on the Website.

30. As a result, even after Plaintiff's contractual relationship with MMMI was terminated, the MMMI network and Website continued to actively provide access to Plaintiff's PII, photos and profiles without her authorization and consent.

B. Value of PII to Hackers and Lack of Segregation of PII Data

31. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it is less protected and regulated than payment card data.

32. Network segmentation of, or isolating (segmenting), the PII data from the remainder of MMMI'S network was not done. Segregation is recommended because, among other reasons, "[i]t's not just cardholder data that's important; criminals are also after personally identifiable information (PII) and corporate data." See Verizon 2014 PCI Compliance Report, available at http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf (hereafter "2014 Verizon Report"), at 54.

33. As noted in the 2014 Verizon Report, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users." Id. Similarly, in the Target data breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 customers. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." Id. Illicitly obtained PII and PCI, sometimes aggregated from different data breaches, is sold on the black market, including on websites, as a product at a set price. See, e.g., <http://krebsonsecurity.com/2011/11/howmuch-is-your-identity-worth> (last visited March 4, 2014).

34. Moreover, PII of individuals with something in common is extremely valuable to criminals because it can help them perpetrate targeted spear phishing attacks. Spear phishers target select groups with something in common, i.e., they are fashion models so that they can send members of the group an email that looks just like an email from a trending designer who

seeks their services. But once recipients click on a link, they can be tricked into downloading malware on their own computers or deceived into giving up additional confidential information such as new passwords, financial information, personal data and much more.

C. Consequences of the Data Breach

35. MMMI failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

36. The ramifications of MMMI'S failure to keep class members' data secure are severe.

37. Plaintiff and proposed class members have suffered injury as a result of MMMI'S conduct. Injuries include:

(i) the loss of the opportunity to control how their PII is used.

(ii) the compromise, publication, and/or theft of their PII.

(iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII.

(iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports;

(vi) the continued risk to their PII, which remains in MMMI'S possession and is subject to further unauthorized disclosures so long as MMMI fails to undertake appropriate and adequate measures to protect the PII of customers and former models in their continued possession.

(vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members;

(viii) the diminished value of Plaintiff's and Class members' PII.

38. The PII lost, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC Interactive Toolkit, Fighting Back Against Identity Theft, available at <http://www.a2gov.org/government/safetyservices/Police/Documents/FTC%20identity%20theft%20guide.pdf> (last visited Jan. 27, 2014).

39. Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. Id. The FTC estimates that as many as 10 million Americans have their identities stolen each year. Id.

40. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud." See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/276 > (last visited Mar. 4, 2014) ("2013 Identity Fraud Report"). 46% of consumers with a breached debit card became fraud victims within the same year. Id.

CLASS ACTION ALLEGATIONS

41. Plaintiff requests relief in her individual capacity and seeks to represent a class consisting of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of classes initially defined as follows:

[a] THE NATIONWIDE CLASS:

All persons residing in the United States, whose personal and/or financial information was disclosed in the data Breach and incursion affecting and reported by MAJOR MODEL MANAGEMENT, INC., on August 25, 2020.

[b] THE NEW YORK SUBCLASS:

All persons residing in New York, whose personal and/or financial information was disclosed in the data breach and incursion affecting and reported by MAJOR MODEL MANAGEMENT, INC., on August 25, 2020.

42. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

43. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

44. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is approximately 500 individuals.

45. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether MMMI and Plaintiff and Class members had a contract for MMMI to protect Plaintiffs' and Class members' PII from unauthorized disclosure to third parties.
b. Whether MMMI breached its contract to protect its users' PII.
c. Whether and when MMMI learned of the Data Breach and whether its response was adequate.
d. Whether MMMI owed a duty to the Class to exercise due care in collecting, storing,

safeguarding and/or obtaining their PII.

e. Whether MMMI breached that duty.

f. Whether MMMI acted unfairly, unlawfully, deceptively, or fraudulently with respect to the Data Breach and representations about its data protection.

g. Whether MMMI implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII.

h. Whether MMMI acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII.

i. Whether MMMI misrepresented the safety and security of its computer systems and networks, particularly the security of PII obtained, maintained, and stored on MMMI'S networks.

j. Whether MMMI'S misrepresentations concerning the safety and security of its computer systems and networks were material with regard to storing, maintaining, and safeguarding Plaintiff's and Class members' PII.

k. Whether MMMI concealed from Plaintiff and Class members crucial information about its inadequate data security measures.

l. Whether MMMI knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII.

m. Whether MMMI unlawfully used, maintained, lost, or disclosed Class members' PII.

n. Whether MMMI unreasonably delayed in notifying affected current and former contracted models of the data breach.

o. Whether MMMI caused Plaintiff and Class members damages; and

p. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

46. Typicality: Plaintiff's claims are typical of those of other Class members because all had their PII compromised accessed as a result of the Data Breach, due to MMMI" S misfeasance.

47. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

48. Superiority and Manageability: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, MMMI'S misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

49. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because MMMI has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

50. Likewise, issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether MMMI owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII.
b. Whether MMMI breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII.
c. Whether MMMI failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security.
d. Whether an implied contract existed between MMMI and the Class members and the terms of that implied contract.
e. Whether MMMI breached the implied contract.
f. Whether MMMI adequately, and accurately informed Class members that their PII had been compromised.

g. Whether MMMI failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

h. Whether MMMI engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class members; and,

i. Whether Class members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of MMMI'S wrongful conduct.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
[NEGLIGENCE]

51. Plaintiff incorporates the above allegations as if fully alleged herein.

52. MMMI owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, deleting, securing, and protecting their PII from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

53. More specifically, this duty included, among other things: (a) designing, maintaining, and testing MMMI'S security systems to ensure that Plaintiff's and class members' personal information was adequately secured and protected; (b) implementing adequate and effective processes to detect an intrusion into their information systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding network intrusions; and (d) maintaining data security measures at least consistent with industry standards.

54. MMMI'S duty to use reasonable care arose from several sources, including those described below.

55. MMMI had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and class members were the foreseeable and probable victims of MMMI'S inadequate security practices. Not only was it foreseeable that Plaintiff and class members would be harmed by the failure to protect their personal information (because hackers routinely attempt to steal such information and use it for nefarious purposes), MMMI knew Plaintiff and the class members probably would be harmed.

56. MMMI'S duty to safeguard Plaintiff's and the class members' PII is also buttressed by N.Y. General Business Law § 899-aa, which was enacted to protect individuals from improper disclosure of their personal information through inadequate data security.

57. MMMI also had a duty to timely notify Plaintiff and class members of the data breach, so they could take appropriate prophylactic and mitigation measures, including freezing their credit, purchasing adequate identity theft protection products, monitoring their accounts even more carefully for unauthorized charges, and cancelling or changing usernames and passwords for compromised accounts,

58. MMMI negligently breached the duties they owed to Plaintiff and class members described above.

59. MMMI breached these duties by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Plaintiff's and class members' PII.

60. MMMI breached these duties by failing to exercise reasonable care and to detect the breach while it was ongoing.

61. MMMI breached these duties by failing to exercise reasonable care and to maintain security systems consistent with industry standards.

62. MMMI breached these duties by failing to exercise reasonable care to disclose that Plaintiff's and the class members' personal information in MMMI'S possession had been or was reasonably believed to have been, stolen or compromised.

63. Plaintiff's and class members' PII would not have been compromised but for MMMI'S wrongful and negligent breach of its duties, as described above.

64. As a direct and proximate result of Defendants' negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and statutory damages, in an amount to be proven at trial.

65. Plaintiff's and class members' injuries include: costs stemming from the use of their PII and the diminution in its value as a result of the Data Breach; costs associated with the detection and prevention of identity theft, including purchasing credit monitoring and identity theft protection services; costs related to the loss of use of and access to their funds; adverse effects on their credit; costs associated with time spent and the loss of productivity from addressing the actual and future consequences of the data breach; and the continued risk of exposure to hackers and thieves of their personal information, which remains in MMMI'S inadequately secured systems.

SECOND CAUSE OF ACTION
[BREACH OF CONTRACT]

66. Plaintiff incorporates the above allegations as if fully alleged herein.

67. Plaintiff and Class members entered into a contract with MMMI whereby MMMI was engaged as their sole and exclusive personal manager in New York in connection with the development of Plaintiffs' careers in modeling, advertising, licensing, and entertainment.

68. Plaintiff and class members were given express and implied assurances of MMMI's code of conduct and that the terms of the contract would adhere to industry standards, with reasonable and practical measures taken, at all times, that their PII data would be protected.

69. Plaintiff and Class members met all or substantially all of their contractual obligations, including providing MMMI with certain PII disclosures required as a material term and condition of the contract.

70. Plaintiff and class members were required, on an annual basis, to pay MMMI for the placement of their photos and model portfolio on MMMI'S Website.

71. MMMI enjoyed the financial benefits of its Website advertising platform which featured photos and profiles of its models.

72. MMMI failed to perform its obligations under the contract, including by failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff's and Class member's PII.

73. MMMI failed to take reasonable steps to ensure that their IT employees or outside vendors used safe and secure systems to protect all PII.

74. MMMI failed to ensure that their contractors had appropriate security protocols and measures in place to protect PII.

75. MMMI allowed their agents, servants, and employees to disclose Plaintiff's PII to unauthorized third parties.

76. MMMI failed to promptly alert or give notice of the breach to Plaintiff and class members.

77. As a direct and proximate result of MMMI'S breach of contract, Plaintiff and Class members did not get what they had bargained for; to wit, that MMMI would take reasonable and practical measures, at all times, to protect their PII.

78. Plaintiff and Class members were damaged in an amount at least equal to the difference in value between that which was promised and the negligent/legally deficient services they actually received from MMMI.

79. As a proximate result of MMMI'S failure to provide its privacy and security services competently and using reasonable care, Plaintiff and Class members have suffered injuries, including, (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in MMMI'S possession and is subject to further unauthorized disclosures so long as MMMI fails to undertake appropriate and adequate measures to protect the PII of current and models in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members; (ix) the diminished value of Plaintiffs' and Class members' PII, and (x) expectation damages.

THIRD CAUSE OF ACTION
[N.Y. GEN. BUS. LAW § 349, et. seq.]

80. Plaintiff incorporates the above allegations as if fully alleged herein.

81. MMMI engaged in deceptive acts or practices in the conduct of its business, trade, and commerce, or furnishing of services, in violation of N.Y. Gen. Bus. Law § 899-bb, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and class members' PII after they terminated their contractual relationship with MMMI.

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and class members' PII, including by implementing and maintaining reasonable security measures.

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and class members' PII.

82. MMMI'S representations and omissions were material because they were likely to deceive reasonable consumers, i.e. individuals seeking to engage exclusive personal managers in New York in connection with the development of their careers in modeling, advertising, licensing, and entertainment, about the adequacy of MMMI'S data security and ability to protect the confidentiality of consumers' PII.

83. MMMI violated the NYS Information Security Breach and Notification Act, which is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law.

84. MMMI violated General Business Law section 899-aa [2], which provides:

> 2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

85. N.Y. Gen. Bus. Law § 899-bb [2] provides as follows:

> 2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data.

86. N.Y. Gen. Bus. Law § 899-bb[2][d] provides as follows:

> (d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter…

87. MMMI acted intentionally, knowingly, and maliciously to violate New York's General Business Law, § 349 and recklessly disregarded Plaintiffs' and class members' rights.

88. As a direct and proximate result of MMMI'S deceptive and unlawful acts and practices, Plaintiff and class members have suffered and will continue to suffer injury and ascertainable losses as follows:

(i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,

detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in MMMI'S possession and is subject to further unauthorized disclosures so long as MMMI fails to undertake appropriate and adequate measures to protect the PII of current and models in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members; (ix) the diminished value of Plaintiffs' and Class members' PII.

89. MMMI is liable to Plaintiff and Class members for compensatory damages available under New York General Business Law, § 349 et. seq.

90. MMMI is liable to Plaintiff and Class members for statutory damages available under New York General Business Law, § 349 et. seq.

91. Pursuant to New York General Business Law, § 349 et. seq., MMMI is liable to pay costs to Plaintiffs and Class members, including reasonable attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class.

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

C. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined.

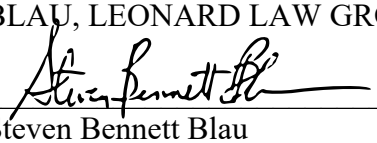
D. For an award of punitive damages.

E. For an award of costs of suit and attorneys' fees, as allowable by law; and

F. Such other and further relief as this court may deem just and proper.

Dated: August 27, 2020

BLAU, LEONARD LAW GROUP, LLC



Steven Bennett Blau
Shelly A. Leonard
23 Green Street, Suite 105
Huntington, NY 11743
(631) 458-1010
sblau@blauleonardlaw.com
sleonard@blauleonardlaw.com

Attorneys for Plaintiff

DEMAND FOR PRESERVATION

PLEASE TAKE NOTICE that MAJOR MODEL MANAGEMENT, INC., ("Defendant') is under a legal duty to maintain, preserve, retain, protect, and not destroy any and all evidence, documents and data, both electronic and hard copy, and/or tangible items pertaining or relevant to property discoverable regarding to all of the claims made in this litigation.

This notice applies to Defendants' on- and off-site computer systems and removable electronic media, plus all computer systems, services, and devices (including all remote access and wireless devices) used for your overall operation. This includes, but is not limited to, e-mail and other electronic communications; electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files, deleted files, cache files, user information, and other data. Further, this notice applies to archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail, and other data. All operating systems, software, applications, hardware, operating manuals, codes keys and other support information needed to fully search, use, and access the electronically stored information.

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging).
- Word processed documents (e.g., Word or WordPerfect documents and drafts).
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets).
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files).
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images).
- Sound Recordings (e.g., .WAV and .MP3 files).
- Video and Animation (e.g., .AVI and .MOV files).
- Databases (e.g., Access, Oracle, SQL Server data, SAP).
- Contact and Relationship Management Data (e.g., Outlook, ACT!).
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools).
- Online Access Data (e.g., Temporary Internet Files, History, Cookies).
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs.

- Project Management Application Data.
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO)

Defendant is directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity, or other criteria.
- Using data or media wiping, disposal, erasure, or encryption utilities or devices.
- Overwriting, erasing, destroying, or discarding back up media.
- Re-assigning, re-imaging, or disposing of systems, servers, devices, or media.
- Running antivirus or other programs effecting wholesale metadata alteration.
- Releasing or purging online storage repositories.
- Using metadata stripper utilities.
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

In order to assure that your obligation to preserve documents and things will be met, please forward a copy of this letter to any and all persons and entities with custodial responsibilities for the items referred to herein. Notify all individuals and affiliated organizations of the need and duty to take the necessary affirmatives steps to comply with the duty to preserve evidence.

Specifically, you are instructed not to destroy, disable, erase, encrypt, alter, or otherwise make unavailable any electronic data and/or evidence relevant to potential claims and to take reasonable efforts to preserve such data and/or evidence.